NASA Procedural Requirements

NPR 1382.1B
Effective Date: July 26, 2022
Expiration Date: July 26, 2027

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

NASA Privacy Procedural Requirements

Responsible Office: Office of the Chief Information Officer

Table of Contents

Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Privacy Management

1.1 Overview
1.2 Roles and Responsibilities

Chapter 2. Identify

2.1 Overview
2.2 Inventory
2.3 Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA)

Chapter 3. Govern

3.1 Overview
3.2 Awareness and Training
3.3 Privacy Accountability
3.4 Privacy Complaints
3.5 Privacy Consequences

3.6 Privacy Redress and Privacy Act Information Requests
3.7 Privacy Rules of Behavior
3.8 Risk Management Strategy

Chapter 4. Control

4.1 Overview
4.2 Collection of Personally Identifiable Information (PII) and sensitive PII

Chapter 5. Communicate

5.1 Overview
5.2 Computer Matching Agreements
5.3 Childrens Online Privacy Protection Act Notice
5.4 Privacy Act Statements
5.5 Privacy Act System of Records Notices
5.6 Privacy Notice
5.7 Web Measurement and Customization Technology Use and Notice

Chapter 6. Protect

6.1 Overview
6.2 Privacy and Information Security
6.3 Privacy Incident Response and Management

Appendix A. Definitions
Appendix B. Acronyms
Appendix C. Requirements Matrices

Preface

P.1 Purpose

a. The purpose of this document is to set forth the procedural requirements for safeguarding individual privacy through the protection of personally identifiable information (PII). PII which is collected, used, maintained, and disseminated by the National Aeronautics and Space Administration (NASA) will be protected regardless of format.

b. This NASA Procedural Requirement (NPR) is based on Federal requirements as listed in Section P.4, Applicable Documents and Forms.

P.2 Applicability

a. This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.

b. For the purposes of this NPR, NASA Headquarters is regarded as a Center. Further, all stipulated Center requirements apply to NASA Headquarters.

c. This directive applies to contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the contracts, grants, or agreements. This directive is applicable to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), only to the extent specified in the NASA/Caltech Prime Contract.

d. This directive applies to PII collected, stored, used, processed, disclosed, or disseminated in any format for use by or on behalf of NASA and includes PII collections that are maintained externally through a contract, outsourced to, or operated by:

(1) Government-owned, contractor operated (GOCO) facilities;

(2) Partners under the National Aeronautics and Space Act; 51 U.S.C. § 20101, et seq;

(3) Partners under the Commercial Space Launch Act, as amended, 51 U.S.C. § 50913;

(4) Partners under cooperative agreements; or

(5) Commercial or university facilities.

e. External collections that are not gathered on behalf of NASA or are merely incidental to a contract (e.g., PII in a contractor's payroll and personnel management system) are excluded from this NPR and are considered non-NASA data.

f. This NPR does not apply to PII collected or maintained by NASA employees and contractors for personal use (e.g., contact information for family, relatives, and doctors), as allowed under NASA Interim Directive (NID) 2540.138, Acceptable Use of Government Furnished Information Technology Equipment, Services, and Resources.

g. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should"

denotes a good practice and is recommended but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

h. In this directive all document citations are assumed to be the latest version unless otherwise noted. Documents cited as authority, applicable, or reference documents may be cited as a different categorization, which characterizes its function in relation to the specific context.

i. In this directive, the citation “Privacy Act of 1974, 5 U.S.C. § 552a” will be referred to as “Privacy Act” throughout.

P.3 Authority

a. The National Aeronautics and Space Act, 51 United States Code (U.S.C.), § 20101 et seq.

b. The E-Government Act of 2002, 44 U.S.C. § 3604 et seq.

c. Privacy Act of 1974, 5 U.S.C. § 552a.n

d. NPD 1382.17, NASA Privacy Policy

e. NPR 2810.1, Security of Information and Information Systems.

f. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations.

P.4 Applicable Documents and Forms

a. Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, 5 U.S.C. § 101.

b. Plain Writing Act of 2010, 5 U.S.C. § 301.

c. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506.

d. Applicability to National Security Systems, 40 U.S.C. § 11103(a).

e. Paperwork Reduction Act (PRA), 44 U.S.C. § 3501 et seq.

f. Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 et seq.

g. Management and Promotion of E- Government Services, 44 U.S.C. § 3601

h. Social Security Number Fraud Prevention Act of 2017, 10 CFR spt. 9.301.

i. Privacy Act NASA Regulations, 14 CFR pt. 1212.

j. Protection of Privacy and Freedom of Information, 48 CFR pt. 24.

k. Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource (7/28/2016).

l. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (09/30/2003).

m. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy (02/11/2005).

n. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information (05/22/2006).

o. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (07/12/2006).

p. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (05/22/2007).

q. OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (06/25/ 2010).

r. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (06/25/2010).

s. NIST SP 800-122, Guide for Protecting the Confidentiality of Personally Identifiable Information (PII).

t. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

u. NASA FAR Supplement 1824.1, Protection of Individual Privacy (09/2015).

v. NID 2540.138, Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources.

w. NPR 1600.1, NASA Security Program Procedural Requirements

x. NPR 8000.4, Agency Risk Management Procedural Requirements.

y. NPR 2810.7, Controlled Unclassified Information.

z. NRRS 1441.1, NASA Records Retention Schedules.

aa. ITS-HBK-1382.03-01, Privacy - Collections, PIAs, and SORNs.

bb. ITS-HBK-1382.03-02, Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.

cc. ITS-HBK-1382.04, Privacy and Information Security Overview.

dd. ITS-HBK-1382.05, Privacy Incident Response: Breach Response Team Checklist and Management.

ee. ITS-HBK-1382.06, Privacy Notice and Redress—Web Privacy and Written Notice, Complaints, Access, and Redress.

ff. ITS-HBK-1382.07, Privacy Awareness and Training.

gg. ITS-HBK-1382.08, Privacy Accountability.

hh. ITS-HBK-1382.09, Privacy Rules of Behavior and Consequences.

ii. ITS-HBK-2810.03, Planning.

jj. ITS-HBK-2810.06, IT Security Awareness, Training and Education.

kk. ITS-HBK-2810.09, Incident Response and Management.

ll. ITS-HBK-2810.11, Media Protection and Sanitization.

P.5 Measurement/Verification

a. Measurement for this policy is determined by Federal regulatory and NASA privacy requirements. These measurements are based upon NASA's privacy goals and the objectives outlined by the Senior Agency Official for Privacy (SAOP).

b. The SAOP provides assessments and evaluations that consist of periodic reporting from the Centers and collecting information for the satisfaction of OMB and Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 reporting requirements.

c. All entities in P.2 of this policy are subject to privacy compliance reviews and evaluations by NASA.

P.6 Cancellation

NPR 1382.1, NASA Privacy Procedural Requirements, July 10, 2013.

Chapter 1 Privacy Management

1.1 Overview

1.1.1 On January 16, 2020, the NIST published the Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. The structure of Privacy Framework follows the Cybersecurity Framework.

1.1.2 NASA is committed to protecting the privacy of personal information of individuals from whom it collects, maintains, uses, and/or disseminates such information.

1.1.3 The NIST Privacy Framework establishes a basic set of activities and outcomes encapsulated in three components: the core, profiles, and implementation tiers.

1.1.3.1 The core is composed of a set of functions, categories, and subcategories which work together to enable a dialogue about managing privacy risk.

a. Functions represent the highest level of categorization for privacy activities. The chapters in this directive align to the functions of the framework, which are:

(1) Identify—Activities and policies that help NASA to understand the scope of both the privacy information and the systems processing privacy information, with a goal of managing privacy risk for individuals.

(2) Govern—Requirements relating to the development and implementation of NASA governance structures to enable an understanding of NASA's risk management priorities and how the priorities are informed by privacy risk.

(3) Control—Requirements for activities to enable NASA to manage data to address privacy risks.

(4) Communicate—Requirements for activities that enable NASA to engage in dialogue about how data are processed and associated privacy risks.

(5) Protect—Requirements for activities relating to data processing safeguards.

b. Categories represent the subdivision of activities under functions.

c. Subcategories representing specific outcomes of technical and/or management activities.

1.1.3.2 Privacy goals and objectives are identified and governed by NASA’s Privacy Program Plan maintained by the Chief Privacy Officer.

1.2 Roles and Responsibilities

1.2.1 This section contains overarching roles and responsibilities related to NASA's entire privacy program. Roles and responsibilities related to specific elements of the privacy program are referenced throughout the remainder of this NPR in their respective chapters.

1.2.1.1 NASA Headquarters, Centers, satellite and component facilities, and support service contractor sites may use internal organizational structure to fulfill the roles and responsibilities

described herein.

1.2.2 Throughout this document, roles and responsibilities are generally listed at the highest level possible, with the assumption that specific tasks and functions may be delegated unless explicitly prohibited, (e.g., a conflict of interest or separation of duties is created).

1.2.2.1 The NASA Administrator shall:

a. Ensure the protection of PII within NASA's information and information systems.

b. Assign a SAOP, who maintains the Agency's privacy program and its overall objectives and priorities.

1.2.2.2 The NASA CIO shall:

a. Provide guidance to the SAOP.

b. Update NPD 1382.17, NASA Privacy Policy, to ensure NASA is current with changes in Federal privacy policy.

1.2.2.3 The SAOP shall:

a. Provide overall responsibility and accountability for ensuring NASA's implementation of privacy information protections.

b. Ensure that NASA is compliant with applicable Federal laws, regulations, policies, guidelines, and NASA privacy program requirements.

c. Develop and maintain a NASA-wide privacy program.

d. Develop, maintain, and monitor NASA privacy goals and objectives.

e. Approve handbooks related to this NPR.

f. Assign a Chief Privacy Officer (CPO) to oversee the NASA-wide privacy program. The Chief Privacy Officer was formerly called the Privacy Program Manager.

g. Assign a NASA Privacy Act Officer (PAO) responsible for oversight of NASA's compliance with the Privacy Act of 1974, 5 U.S.C. § 552a.

h. Advise senior NASA officials concerning their responsibilities to protect privacy information.

i. Evaluate legislative, regulatory, and other guidelines and policies related to privacy.

j. Ensure that a Privacy Threshold Analysis (PTA) is conducted for any new, or significantly changed, applications, w websites, information systems (including third party applications and information systems and collections of information provided for by external service providers who are collecting information on behalf of NASA), and all non-electronic information collections to determine whether there are any privacy implications or other regulatory compliance requirements. Guidance for conducting PTAs is in ITS-HBK-1382.03-01, Privacy- Collections, PIAs, and SORNs.

k. Ensure when initial assessments via the PTA process calls for the completion of a full Privacy Impact Assessment (PIA), one will be initiated and completed, in accordance with ITS-HBK-1382.03-01, prior to actively collecting any information.

l. Reviews and approves PIAs.

1.2.2.4 The Senior Agency Information Security Officer (SAISO) shall provide necessary management and resources in support of the NASA-wide privacy program as established by the SAOP.

1.2.2.5 The NASA CPO shall:

a. Oversee and manage the development and implementation of policy and procedure, guidance, directives, and requirements for NASA in support of compliance with Federal laws, statutes, and Government-wide policy as directed by the SAOP.

b. Ensure that NASA complies with privacy requirements within Federal statutes listed in this directive, including the collection, maintenance, use, and dissemination of privacy information.

c. Develop and maintain NASA privacy policies, procedural requirements, and handbooks as directed by the SAOP.

d. Establish Agency requirements and processes for conducting PTAs and PIAs for new or significantly changed applications, w websites, or information systems, and make PIAs publicly available (unless public release is otherwise prohibited).

e. Oversee and provide guidance in the implementation and the day-to-day operation of the NASA-wide privacy program as directed by the SAOP.

f. Review NASA's compliance with information privacy laws, regulations, and policies annually to validate effectiveness and ensure conformity with current Federal policies and guidance as directed by the SAOP.

1.2.2.6 The NASA Privacy Act Officer shall:

a. Ensure compliance with requirements of the Privacy Act.

b. Oversee, manage, and implement the Privacy Act requirements for NASA.

1.2.2.7 The Center/Executive Director shall:

a. Appoint a Center Privacy Manager (CPM).

b. Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy.

1.2.2.8 The Center CIO shall:

a. Ensure that all Center information and information systems comply with the provisions of this NPR.

b. Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy.

c. Support the CPM in protecting PII and/or Information in Identifiable Form (IIF) at the Center.

d. Ensure that Information Owners (IOs), Information System Owners (ISOs), and Data Owners (DOs) assess the privacy aspects of information collections and information systems for which they are responsible and ensure all required security safeguards are implemented in accordance with current NASA policy and procedural requirements for the collection, use, maintenance, and

dissemination of personal information.

1.2.2.9 The Center Chief Information Security Officer (CISO) shall support the CPM in protecting PII at the Center.

1.2.2.10 The CPM shall:

a. Serve as the Center advisor to the Center Director, Center CIO, Center CISO, and Information System Owners (ISOs) on all matters pertaining to privacy.

b. Function as the primary Center point of contact/liaison to the NASA CPO and NASA PAO.

c. Work with ISOs to review and aid in ensuring compliance with all privacy requirements, as needed.

d. Validate the proper disposition and/or sanitization process for files and records (paper, electronic, or other media formats), which contain privacy information.

e. Ensure the NASA privacy program is implemented at the Center in accordance with NASA policy.

f. Ensure that IOs, ISOs, and DOs perform the required information collection assessments (i.e., PTAs and PIAs) and aid in the development of any additional documentation indicated as required upon completion of the PTA (or PIA if required). (This includes SORNs, Federal Register notices, and Privacy Act Statements.)

g. Serve as their Center's liaison for the controlled unclassified information (CUI) program unless a different liaison is identified by the Center's leadership.

1.2.2.11 Contracting Officers (COs) or Agreement Managers shall ensure that the requirements of this directive are included and in scope for all NASA contracts, agreements under 51 U.S.C. § 20101, cooperative agreements, partnership agreements, or other agreements pursuant to which privacy information (e.g., PII, PHI, PAI) is being collected, processed, stored, or transmitted.

1.2.2.12 The ISO shall:

a. Acquire, develop, integrate, operate, modify, maintain, and dispose of information systems containing PII in a manner consistent with Federal statutes, regulation, and NASA privacy policies.

b. Ensure compliance with the Privacy Act for applications and information systems.

c. Verify with the CO/Contracting Officer Representative (COR) that any contract that requires the operation of a System of Records (SOR) on behalf of NASA includes the clauses required per Protection of Privacy and Freedom of Information, 48 CFR pt. 24.

d. Notify the CO when purchase requests include services covered by the Privacy Act or Paperwork Reduction Act (PRA), 44 U.S.C. § 3501 et seq.

e. Notify the CO when contractor services will require or include access to PII collected by or on behalf of NASA.

f. Verify that the contract statement of work identifies this NPR as outlining the NASA-specific requirements to be followed by the contractor.

1.2.2.13 The NASA User shall:

a. Comply with all Federal laws, statutes, and NASA privacy policies and procedures in this and the referenced documents.

b. Protect all PII in the user's custody (whether virtual, electronic, actual, or otherwise) from unauthorized disclosure, use, modification, or destruction so that the confidentiality, integrity, and availability of the information are preserved.

Chapter 2 Identify

2.1 Overview

2.1.1 The Identify chapter ensures NASA's compliance with NIST requirements for the inventory and assessment of PII.

2.1.2 NASA is responsible for assessing the PII it collects and notifying individuals of what information is collected, why it is being collected, and how the information will be used.

2.1.3 In accordance with the Privacy Act, The E-Government Act of 2002, 44 U.S.C. § 3604, and OMB requirements, NASA uses compliance documentation such as PTAs, PIAs, and System of Records Notices (SORNs), which are discussed in Chapter 5. These tools assist NASA in identifying and reducing the privacy risks related to NASA's activities, notifying the public of privacy impacts, and determining which steps to take to mitigate potential impacts to personal privacy.

2.1.4 All NASA applications, information systems, and websites are to be reviewed via the PTA process to determine whether they require a PIA.

2.1.5 NASA Privacy Risk Management and Compliance procedures are governed by ITS-HBK-1382.03-01.

2.2 Inventory

2.2.1 Overview

2.2.1.1 Inventories are essential to NASA's understanding management of privacy risk.

2.2.1.2 A thorough understanding of the scope of NASA's collection of PII provides visibility into scope of privacy information.

2.2.2 Procedural Requirements

2.2.2.1 The SAOP shall:

a. Ensure the establishment and maintenance of the NASA Master Privacy Information Inventory (MPII).

b. Work with the SAISO to ensure the information system inventory required by NPR 2810.1, Security of Information and Information Systems, includes information on data processing systems processing PII.

2.2.2.2 The CPM shall ensure the MPII established per section 2.2.2.1a accurately reflects all electronic and non-electronic collections of information for their respective Center and is current.

2.3 Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA)

2.3.1 Overview

2.3.1.1 PTAs and PIAs are part of a formal process that NASA uses to analyze how information is processed by an information system, application, or website to ensure that NASA's handling conforms to applicable statutory, regulatory, and policy requirements for privacy information identified in this directive.

2.3.1.2 The PIA is used to determine the risks and effects of collecting, maintaining, and disseminating IIF on members of the public. NASA conducts PIAs under two circumstances:

a. In accordance with 44 U.S.C. § 3604 and NIST SP 800-53, for any new or substantially changed information system that collects, maintains, or disseminates IIF from or about members of the public, (under 44 U.S.C. § 3604, members of the public exclude Government personnel, contractors, and partners); or

b. For a new collection of ten or more members of the public in accordance with 44 U.S.C. § 3501.

2.3.1.3 A PIA describes:

a. The information to be collected.

b. The purpose of the collection (why it is collected).

c. The intended use collection.

d. With whom the information will be shared.

e. Whether the information was collected with the consent of the owner (or the owner's parent or guardian, if needed, in accordance with Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506.

f. How the information will be secured.

g. Whether a SOR is created under the Privacy Act.

2.3.1.4 In addition, the PIA examines and documents the evaluation of protections and alternative processes for handling information to mitigate potential privacy risks.

2.3.1.5 Unless otherwise prohibited, NASA is responsible for posting the PIA publicly.

2.3.1.6 NIST SP 800-53 PL-5, Information Security Controls, is governed at NASA by ITS-HBK-2810.03, Planning, and ITS-HBK-1382.03-01.

2.3.1.7 Information on how to conduct a PTA and PIA: review, approval, publication requirements, and the relationship to 44 U.S.C. § 3501 and the Privacy Act are governed by ITS-HBK-1382.03-01.

2.3.2 Procedural Requirements

2.3.2.1 The SAOP shall:

a. Establish Agency policy, requirements, and process for conducting PTAs and/or PIAs for new or revised applications and information systems to limit the identification of individuals.

b. Assess the impact of technology on privacy and the protection of personal information.

c. Evaluate and approve or disapprove all completed PIAs.

d. Ensure that data is disposed of at the Agency level according to NRRS 1441.1, NASA Records Retention Schedules and NPR 2810.7, Controlled Unclassified Information.

2.3.2.2 The Center CIO shall ensure that a PTA, and when needed a PIA, is conducted for every application and information system, including websites.

2.3.2.2 The NASA CPO shall:

a. Implement Agency policy, requirements, and processes for conducting PTAs and PIAs for new or revised applications and information systems.

b. Ensure PIAs are thorough and meet all applicable standards.

c. Ensure that completed PIAs are made publicly available for applications and information systems, including websites, which collect and/or maintain IIF on members of the public, consistent with Federal policy, unless otherwise prohibited.

2.3.2.3 The CPM shall:

a. Assist ISOs in the completion of PTAs and, when needed, PIAs.

b. Conduct timely reviews of applications and information systems, including websites, PTAs, and PIAs to ensure the ISO has addressed adequate protection of privacy and/or Privacy Act information (PAI).

c. Ensure the ISOs update PTAs and, when needed, PIAs.

d. Conduct annual PIA reviews.

e. Ensure procedures exists to dispose of data at the Center level according to NRRS 1441.1, NPR 2810.1, and NPR 2810.7.

2.3.2.4 The ISO shall:

a. Ensure that a PTA is conducted and approved for the applications and information systems, including websites, under the ISO’s purview.

b. Ensure that a PIA is reviewed and approved for:

(1) An information system that collects, maintains, or disseminates IIF from or about members of the public; or

(2) An electronic collection of IIF for ten or more individuals, consistent with 44 U.S.C. § 3501.

c. Ensure that they conduct a re-evaluation of PTAs and, when needed, PIAs following significant modifications to all applications and information systems, including websites.

d. Ensure that a PIA is conducted prior to use of a third-party website or application that collects PII.

e. Review completed PTAs and PIAs annually to ensure ongoing accuracy.

Chapter 3 Govern

3.1 Overview

The Govern chapter describes NASA's governance structures to understand, manage, and prioritize privacy risk.

3.2 Awareness and Training

3.2.1 Overview

3.2.1.1 The Privacy Awareness and Training section relates to NASA's initiatives to ensure that all NASA Users are aware of and trained on their roles and responsibilities related to PII.

3.2.1.2 Several OMB documents outline the privacy training requirements, including OMB Circular A-130, Managing Information as a Strategic Resource, OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy (02/11/2005), and OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (05/22/2007). Specifically, OMB M-07-16 requires that NASA is responsible for providing training to every user prior to them gaining access to NASA information and information systems, with a requirement for annual refresher training thereafter. Additionally, advanced training may be required depending on the privacy-related responsibilities of the NASA user.

3.2.1.3 NASA Privacy Training and Awareness procedures are governed by ITS-HBK-1382.07, Privacy Awareness and Training, and ITS-HBK-2810.06, IT Security Awareness, Training and Education.

3.2.2 Procedural Requirements

3.2.2.1 The SAOP shall:

a. Ensure NASA users complete training and education on their privacy responsibilities, including acceptable rules of behavior, when and how to report privacy related incidents, and consequences for violating this NPR.

b. Oversee the mandatory annual privacy training program.

c. Oversee a privacy awareness program.

3.2.2.2 The NASA CPO shall:

a. Review and approve all privacy awareness and training materials.

b. Develop privacy awareness and training materials.

c. Work with the Information Technology Security Awareness and Training Center (ITSATC) to ensure privacy awareness and training materials meet information security training requirements.

d. Ensure the privacy training:

(1) For the NASA user explains the policies and procedures for safeguarding PII collected and maintained at NASA.

(2) For the NASA user explains the privacy rules of behavior and consequences.

(3) For the NASA user with access to NASA data, explains that willful disclosure of information to individuals not entitled to Privacy Act records or sensitive privacy information in any form is strictly prohibited.

(4) For persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record within any SOR, explains the requirements regarding the protection, use, and release of the Privacy Act records.

(5) For persons involved in the design, development, operation, or maintenance of any PII collection, explains the requirements regarding the protection, use, and release of the records.

e. Determine the annual training requirements for CPMs.

3.2.2.3 The CPM shall:

a. Complete privacy role-based training, as required.

b. Ensure awareness and training programs are conducted at the Center level.

3.2.2.4 The ISO shall:

a. Ensure that all NASA users who have access to PII or who develop or supervise procedures for handling PII are trained and are compliant with policies and procedures in NPD 1382.17, this directive, and referenced documents for safeguarding PII collected and maintained at or on behalf of NASA.

b. Ensure that persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record in any SOR, are trained in the requirements regarding the protection, use, and release of the Privacy Act records.

c. Ensure that persons involved in the design, development, operation, or maintenance of any PII collection are trained in the requirements regarding the protection, use, and release of the records.

3.2.2.5 The NASA User shall:

a. Participate in mandatory privacy training prior to gaining access to NASA information and information systems, and yearly thereafter.

b. Participate in privacy role-based training, as required.

3.2.2.6 The Center Breach Response Team (BRT) members shall participate in annual BRT training and exercises.

3.3 Privacy Accountability

3.3.1 Overview

3.3.1.1 The Privacy Accountability section relates to NASA’s initiatives to ensure accountability as related to compliance with applicable privacy protection requirements.

3.3.1.2 This section includes requirements that ensure NASA's compliance with established privacy controls and includes internal reporting requirements and external reporting requirements.

3.3.1.3 NASA Privacy Accountability procedures are governed by ITS-HBK-1382.08-01, Privacy Accountability.

3.3.2 Internal Reporting Procedural Requirements.

3.3.2.1 Overview

a. Internal reporting requirements exist within NASA to internally track compliance with privacy laws, regulations, and NASA's policies and procedures.

b. Internal reporting requirements include metrics, data calls, and status reports.

c. The results of internal reporting requirements are used to create metrics that allow the SAOP and the NASA CPO to evaluate the goals and objectives of the NASA privacy program.

3.3.2.2 The SAOP shall update NASA senior management on the status of Agency performance in meeting privacy goals and objectives.

3.3.2.3 The NASA CPO shall update the SAOP on privacy metrics annually as part of the 44 U.S.C. § 3551 reporting process.

3.3.2.4 The CPM shall:

a. Update the NASA CPO, Center CIO, and Center CISO on the status of meeting the privacy requirements at the Center.

b. Respond to various privacy related mandates and requests for information from the NASA CPO and NASA PAO.

c. Report any Privacy (PII) or the Privacy Act violations to the CPO.

d. Track planned, in progress, and completed corrective actions taken to remedy deficiencies identified in compliance reviews.

e. Ensure the NASA MPII is up to date and accurately reflects all electronic and non-electronic collections of information for their respective Center.

f. Report all significant privacy related activities (e.g., BRT activities and privacy complaints) to the CPO.

3.3.2.5 The ISO shall:

a. Report to the CPM on the status of compliance with NASA Privacy requirements through the PTA and PIA processes accomplished in RISCS.

b. Control disclosures from their SOR and maintain accountings of all disclosures of information in accordance with Privacy Act NASA Regulations, 14 CFR pt. 1212.

3.3.2.6 The NASA User shall report any suspected or confirmed unauthorized disclosures of PII in any form to the Security Operations Center (SOC) in accordance with Agency IT security incident reporting procedures.

3.3.3 External Reporting Procedural Requirements.

3.3.3.1 Overview

NASA has a number of external reporting requirements, including those required by OMB, Department of Homeland Security (DHS), 44 U.S.C. § 3551, Office of the Inspector General (OIG), Government Accountability Office (GAO), and Congressional inquiries. For example, NASA is required to report annually to OMB or DHS under 44 U.S.C. § 3551 on privacy-related issues, including metrics on PIAs and SORNs.

3.3.3.2 The SAOP shall:

a. Ensure external reporting requirements are met.

b. Respond to external reporting requirements.

c. Approve NASA's privacy reports required by OMB and 44 U.S.C. § 3551.

d. Develop and maintain a privacy reviews schedule.

a. Ensure that reviews are conducted as prescribed by the Privacy Act and OMB Circular A-130 and summarized in ITS-HBK-1382.08-01.

3.3.3.3 The NASA CPO shall:

a. Produce and provide NASA's privacy reports required by OMB and 44 U.S.C. § 3551 to the NASA SAISO and the NASA SAOP.

b. Ensure that privacy reviews are conducted in accordance with the schedule outlined in ITS-HBK-1382.08.

3.3.3.4 The NASA PAO shall coordinate and conduct the Privacy Act and OMB Circular A-130 reviews in accordance with the schedule outlined in ITS-HBK-1382.08-01.

3.3.3.5 The CPM shall:

a. Coordinate 44 U.S.C. § 3551 privacy reporting data collection efforts for their Center and report to the NASA CPO, Center CIO, and Center CISO.

b. Coordinate the Privacy Act reviews as directed by the NASA PAO.

3.4 Privacy Complaints

3.4.1 Overview

3.4.1.1 NASA is required by OMB to provide a mechanism for receiving and managing complaints from the public and from NASA users.

3.4.1.2 Specific information on the privacy complaints process is governed by ITS-HBK-1382.06-01, Privacy Notice and Redress—Web Privacy and Written Notice, Complaints, Access, and Redress.

3.4.2 Procedural Requirements

3.4.2.1 The SAOP shall:

a. Ensure policies and processes for filing and managing privacy complaints and inquiries are developed and maintained.

b. Ensure that complaints are recorded, tracked, and addressed.

3.4.2.2 The NASA CPO shall work with the SAOP to record, track, and address privacy complaints.

3.4.2.3 The CPM shall:

a. Receive and seek to address Center-level privacy complaints.

b. Report Center-level privacy complaints to the NASA CPO via the process defined in ITS-HBK-1382.06-01.

3.4.2.4 The ISO shall:

a. Receive and seek to address privacy complaints associated with the application, information system, or website.

b. Report application, information system, or website privacy complaints to the CPM.

3.5 Privacy Consequences

3.5.1 Overview

3.5.1.1 NASA can impose penalties on a NASA user who violates this NPR for privacy related violations. Consequences may range from reprimand to suspension or removal. Specifically, the consequences for violating the privacy-related provisions of this NPR are defined in the Privacy Act, 44 U.S.C. § 3604, and the handbook on rules of behavior identified below.

3.5.1.2 Consequences for privacy-related violations are governed by ITS-HBK 1382.09-01, Privacy Rules of Behavior and Consequences.

3.5.2 Procedural Requirements

3.5.2.1 The SAOP shall outline the consequences and penalty guidelines related to privacy violations.

3.5.2.2 The NASA CPO shall:

a. Advise the SAOP on consequences for violating this NPR.

b. Advise the CPM on consequences for violating this NPR at the Center level.

c. Establish requirements and procedures for reporting known, suspected, or likely violations of the privacy requirements of this NPR.

3.5.2.3 The CPM shall provide support to the CPO to ensure adherence to the requirements of this NPR at the Center level.

3.5.2.4 The ISO shall:

a. Meet publication requirements for Privacy Act SOR. Any official who willfully maintains a Privacy Act SOR without meeting the publication requirements is subject to possible criminal

penalties or administrative sanctions, or both.

b. Be held accountable for privacy violations of this NPR; penalties range from criminal to administrative.

3.5.2.5 The NASA User shall be held accountable for violations of this NPR and related handbooks. Penalties may include reprimand, suspension, removal, or other administrative action, fines, additional privacy training, or other actions in accordance with applicable laws and Agency disciplinary policy.

3.5.2.6 NASA Users may:

a. Be subject to written reprimand, suspension, removal, or other administrative action under the following situations:

(1) Knowingly failing to implement and maintain information security controls required by this NPR for the protection of PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

(2) Failing to report any known or suspected loss of control or unauthorized disclosure of PII.

(3) For managers, failing to adequately instruct, train, or supervise employees in their privacy responsibilities.

b. Be subject to criminal penalties for willful and intentional violations of the Privacy Act.

3.6 Privacy Redress and Privacy Act Information Requests

3.6.1 Overview

3.6.1.1 NASA provides a mechanism for redress and remedy from misuse or mishandling of PII and for correcting inaccuracies. Specifically, NASA provides the public and the NASA user with the opportunity to amend or correct their PII.

3.6.1.2 The redress process is governed by ITS-HBK-1382.06-01.

3.6.1.3 Additionally, NASA responds to the Privacy Act information requests in accordance with 14 CFR pt. 1212.

3.6.2 Procedural Requirements

3.6.2.1 The SAOP shall:

a. Ensure policies and procedures for redressing misuse or mishandling of PII and for correcting inaccuracies are maintained. The SAOP will ensure that the policies follow these guidelines:

(1) In accordance with the Plain Writing Act of 2010, 5. U.S.C. § 301, be in plain language and easy to read and understand.

(2) Explain the right of redress.

(3) Explain the process for complaining, seeking redress, and/or appealing adverse decisions.

(4) Provide a general timeline for the redress process.

(5) Identify the privacy policy related to PII being collected, processed, or maintained.

b. Permit individual access to the Privacy Act SOR in order to amend those Privacy Act records, as permitted in accordance with 14 CFR pt. 1212.

c. In accordance with the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, 5 U.S.C. § 101:

(1) Ensure the ability for NASA to accept remote identity-proofing and authentication for the purposes of allowing an individual to request access to their records or to provide prior written consent authorizing disclosure of their records under the Privacy Act.

(2) Ensure the ability for NASA to accept the access and consent forms from any individual properly identity-proofed and authenticated remotely through digital channels for the purpose of individual access to records for authorizing disclosure of the individual's records to another person or entity, including a congressional office.

3.6.2.2 The NASA CPO shall assist the SAOP in redressing PII issues.

3.6.2.3 The PAO shall provide a Privacy Act record access request process for individuals seeking access to their individual NASA maintained record in 14 CFR pt. 1212.

3.6.2.4 The CPM shall forward any Privacy Act record access requests received to the relevant System Manager for processing in accordance with 14 CFR pt. 1212.

3.6.2.5 The System Manager (the ISO or IO) shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 CFR pt. 1212 and the Privacy Act.

3.6.2.6 The Freedom of Information Act (FOIA) Officer shall process Privacy Act record access requests the Officer receives from an individual seeking access to the individual's NASA maintained record in accordance with 14 CFR pt. 1212 and the Privacy Act in conjunction with the System Manager.

3.7 Privacy Rules of Behavior

3.7.1 Overview

3.7.1.1 Privacy Rules of Behavior include the NASA user responsibilities outlined within the chapters of this NPR and the related handbooks in P.4.

3.7.1.2 Specific information on Rules of Behavior is governed by NID 2540.138, Acceptable Use of Government Office Property Including Information Technology.

3.7.2 Procedural Requirements

3.7.2.1 The SAOP shall:

a. Ensure Rules of Behavior for privacy are outlined within this NPR and maintained in the associated privacy handbook, ITS-HBK-1382.09-01.

b. Ensure that awareness and training materials include information on privacy Rules of Behavior.

3.8 Risk Management Strategy

3.8.1 Overview

3.8.1.1 NPR 2810.1 establishes requirements for cybersecurity risk management strategy to work in conjunction with requirements of NPR 8000.4, Agency Risk Management Procedural Requirements.

3.8.1.2 Management of privacy risk is an important component of NASA's overall risk management strategy and is deeply related to cybersecurity risks.

3.8.2 Procedural Requirements

3.8.2.1 The SAISO shall ensure the Cybersecurity Risk Management Strategy required by NPR 2810.1, includes consideration of privacy risks within the context of the strategy.

3.8.2.2 The CPO shall work with the SAOP and the SAISO to ensure that privacy risk is incorporated into NASA's overall risk management strategies.

Chapter 4 Control

4.1 Overview

4.1.1 The Control chapter relates to NASA's initiatives to manage the scope of data collection and processing in a manner that addresses privacy risks. Integrating privacy controls across multiple control families in NIST SP 800-53 Rev. 5 makes these controls much more visible in the overall assessment, authorization, and continuous monitoring processes for NASA information systems. Refer to ITS-HBK-1382.04.

4.1.2 Control of the collection and processing of privacy-related data is to incorporate privacy principals, such as data minimization and individual participation.

4.1.3 Data minimization is a critical aspect of NASA's efforts to preserve individuals' privacy; while NASA uses technical and policy means to protect sensitive personal information, such means are fallible, and the only assured method of protection is not to collect the information in the first place.

4.1.4 In cases where NASA collects privacy-related data, the means to manage those data are critical to protecting individuals' privacy and the NIST SP 800-53, Rev. 5 control families are critical to achieving those goals.

4.2 Collection of Personally Identifiable Information (PII) and sensitive PII

4.2.1 Overview

4.2.1.1 NASA collects both sensitive and non-sensitive PII and manages that information according to these procedural requirements. The PII of NASA employees and its contractors is sensitive when so assessed through analysis of the data's use and context. Sensitive PII is a subset of PII, which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

4.2.1.2 The collection of PII during official government business is permitted when:

a. Such collection is authorized by law or Executive Order.

b. Federal and NASA privacy requirements are satisfied.

c. Such collection is otherwise necessary to a NASA program and/or its associated mission.

4.2.1.3 Specific information on collecting PII may be found in ITS-HBK-1382.03-01.

4.2.2 Procedural Requirements

4.2.2.1 The Administrator shall ensure, in accordance with Social Security Number Fraud Prevention Act of 2017, 10 CFR spt. 9.301, NASA does not include a social security number (SSN) on any NASA-developed document sent by physical mail unless:

a. The Administrator approves such inclusion; and

b. Inclusion is necessary because:

(1) Inclusion is required by law or regulation.

(2) An SSN is needed to identify a specific individual and no other substitute is available.

(3) Inclusion is needed to fulfill a compelling Agency business need.

4.2.2.2 The SAOP shall:

a. Limit the collection of PII to that which is legally authorized, consistent with Federal and NASA privacy requirements, and to the minimum extent necessary.

b. Ensure that PII is collected only when necessary for the proper performance of NASA's functions and mission support.

c. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

4.2.2.3 The NASA CPO shall coordinate and direct annual NASA-wide review activities to reduce or eliminate unnecessary collections of PII.

4.2.2.4 The CPM shall:

a. Work with ISOs to ensure that all PII is maintained with accuracy, relevance, timeliness, and completeness.

b. Coordinate annual review activities at the Center level with ISOs to ensure PII is collected in accordance with this policy and to reduce or eliminate unnecessary collections of PII.

c. Work with ISOs to eliminate the unnecessary use of SSNs.

4.2.2.5 The ISO shall:

a. Eliminate the collection of information if the information is unnecessary to a NASA program and/or its associated mission.

b. Ensure that all privacy information is maintained with accuracy, relevance, timeliness, and completeness.

c. Ensure that Privacy Act records are collected and maintained in accordance with NASA Privacy Act policies.

d. Conduct annual review activities to reduce or eliminate unnecessary collections of PII.

e. Avoid the collection of SSNs, in accordance with NPD 1382.17, unless required by statute or some other requirement mandating the use of SSNs.

4.2.2.6 NASA Users shall:

a. Not include an SSN on any NASA-developed document sent by physical mail unless the Administrator approves such inclusion in accordance with section 4.2.2.1 of this directive. The process for gaining Administrator approval is governed by the CPO and detailed in ITS-HBK 1382.03-02, Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.

b. Ensure, if ever including an SSN on a NASA-developed document sent by physical mail in

accordance with section 4.2.2.6a of this directive:

(1) Where feasible, the SSN is partially redacted; and

(2) The SSN is not visible on the outside of any such package.

Chapter 5 Communicate

5.1 Overview

5.1.1 The Communicate chapter describes NASA's requirements to ensure notice has been provided to the public and that a mechanism (i.e., policies and procedures) is in place to allow an individual to request information NASA has collected about them and, if needed, to redress or correct their information.

5.1.2 NASA provides general notice to the public in a number of ways, including the publishing of PIAs, SORNs, Privacy Act Statements, and the NASA Web Privacy Policy and Important Notices ("NASA Web Privacy Policy").

5.1.3 NASA Privacy Notice and Redress procedures are governed by 14 CFR pt. 1212 and governed by ITS-HBK-1382.06-01

.

5.2 Computer Matching Agreements

5.2.1 Overview

5.2.1.1 In accordance with the Privacy Act, a computer matching agreement and public notice of the proposed match will be published in the Federal Register before NASA matches any of its SORs with a SOR of another Federal entity or with non-Federal records.

5.2.1.2 Specific information on computer matching agreement requirements is detailed in ITS-HBK-1382.03-01.

5.2.2 Procedural Requirements

5.2.2.1 The NASA SAOP shall:

a. Establish a Data Integrity Board that is responsible for approving, overseeing, and coordinating the matching program before any ISO may engage in a computer matching program as defined by the Privacy Act.

b. Provide guidance on computer matching agreements.

5.2.2.2 The NASA PAO shall work with the ISO to prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.

5.2.2.3 The ISO shall work with the PAO to prepare and ensure publication of a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.

5.3 Children's Online Privacy Protection Act Notice

5.3.1 Overview

5.3.1.1 NASA websites that target children and collect PII from children under age 13 are required to provide conspicuous notice of the information collection practices, verifiable parental consent, and access, as defined by 15 U.S.C. §§ 6501-6506.

5.3.1.2 Specific information on 15 U.S.C. §§ 6501-6506 notice requirements is governed by ITS-HBK-1382.06-01.

5.3.2 Procedural Requirements

5.3.2.1 The CPO shall maintain Agency guidance for compliance with 15 U.S.C. §§ 6501-6506.

5.3.2.2 The ISO shall:

a. Ensure compliance with 15 U.S.C. §§ 6501-6506 for websites intended to be used by, or targeted to, children under the age of 13 that collect PII.

b. Ensure that notice is provided concerning what information is being collected from children by the operator, how the information will be used, and the operator's disclosure practices.

c. Ensure verifiable parental approval is obtained for the collection, use, or disclosure of information from children.

d. Provide a process for parental review of information collected from the child.

e. Provide an opportunity for parental refusal to permit the operator's future use of the information or future collection of information.

f. Provide a means for the parent to obtain the personal information collected from the child.

5.4 Privacy Act Statements

5.4.1 Overview

5.4.1.1 In accordance with the Privacy Act, individuals who are asked to provide information that will be maintained in a NASA Privacy Act SOR are required at the point of collection to be presented with a Privacy Act Statement (hereinafter referred to as a Privacy Act Statement).

5.4.1.2 The Privacy Act Statement requirement may be accomplished through a standalone paper-based statement, a statement on the paper or electronic form, or an electronic statement on a dedicated web page, any one of which may be retained by the individual.

5.4.1.3 Specific information on the form and contents of Privacy Act Statement requirements is governed by ITS-HBK-1382.03-01.

5.4.2 Procedural Requirements

5.4.2.1 The SAOP shall provide guidance on the use of Privacy Act Statements.

5.4.2.2 The NASA PAO shall work with the CPM to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

5.4.2.3 The CPM shall work with ISOs and the PAO to ensure the Privacy Act Statement meets the requirements of the Privacy Act.

5.4.2.4 The ISO shall:

a. Ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are presented at the point of collection with a Privacy Act Statement that:

(1) Is presented either on the information collection sheet or screen, or via a separate sheet or screen that the individuals can print and retain;

(2) Complies with the requirements outlined in 14 CFR pt.1212; and

(3) Is in a format that the individual may be able to retain in a physical or hard copy.

b. Ensure that new NASA forms or Center forms created for the collection of SOR information provide the correct and specific Privacy Act Statement for that SOR.

5.5 Privacy Act System of Records Notices

5.5.1 Overview

5.5.1.1 In accordance with the Privacy Act, a SORN is required for each NASA SOR containing information on individuals from which records are retrieved by an individual identifier (i.e., name of the individual or by some unique number, symbol, or other identifier assigned to an individual), unless the SOR is limited to work-related information, (e.g., work e-mail or work phone number).

5.5.1.2 A SORN is required to be published in the Federal Register prior to any collection or new use of information in a Privacy Act system.

5.5.1.3 Specific information on the review, approval, and publication requirements for a SORN is detailed in ITS-HBK-1382.03-01.

5.5.2 Procedural Requirements

5.5.2.1 The SAOP shall:

a. Provide guidance on the development and publication of SORNs in such way that limits the formulation of inferences about individuals' behavior or activities.

b. Review and issue all SORNs for publication in the Federal Register.

5.5.2.2 The NASA PAO shall:

a. Review and revise draft SORNs in cooperation with the system manager.

b. Coordinate the Agency and OMB reviews of SORNs and obtain SAOP signature for SORN submission to the Federal Register for publication through the NASA Federal Register Liaison Officer.

c. Coordinate with CPMs in determining whether an existing NASA or other government SORN covers Privacy Act records maintained by NASA.

5.5.2.3 The CPM shall:

a. Work with ISOs in identifying the need for a Privacy Act SORN.

b. Assist the ISO in drafting a SORN for publication in the Federal Register, if not already covered

under an existing SORN.

c. Provide the NASA PAO with draft SORNs, as required.

d. Conduct SORN reviews, as required.

e. Coordinate the review and approval of new draft SORNs and Privacy Act notice updates with ISOs and the NASA PAO.

5.5.2.4 The ISO shall:

a. Limit the maintenance of Privacy Act records on individuals that are retrievable by name or other personal identifier to only those instances for which a Privacy Act SORN has been published in the Federal Register.

b. Provide draft content to enable the PAO to complete a SORN for publication in the Federal Register, if not already covered under an existing SORN.

c. Work with the CPM and the NASA PAO to publish a SORN in the Federal Register.

5.6 Privacy Notice

5.6.1 Overview

5.6.1.1 Except as provided in this paragraph, all publicly facing NASA websites are to link to the NASA Web Privacy Policy. This includes websites that are operated under contract that are deemed to be maintained by the Agency and all websites operated on behalf of the Agency. Posting the NASA Web Privacy Policy is not required if:

a. A website contains no “Government information,” as defined in OMB Circular A-130 (i.e., information created, collected, processed, disseminated, or disposed of by or for the Federal Government);

b. A website is an Agency intranet website accessible only by authorized NASA users; or

c. A website is a National Security system, as defined by Applicability to National Security Systems, 40 U.S.C. § 11103(a), or as exempt from the definition of information technology, as defined in Section 202(i) of Management and Promotion of Electronic Government Services, 44 U.S.C. § 3601.

5.6.1.2 In accordance with OMB M-10-23, the NASA Web Privacy policy is to be included on official NASA websites and applications hosted on third-party websites and applications. Specific information on privacy notice requirements is detailed in ITS-HBK-1382.06-01.

5.6.2 Procedural Requirements

5.6.2.1 The NASA CIO shall, subject to the conditions of Section 5.3.2:

a. Ensure the NASA Web Privacy Policy is posted (or linked to) all public facing NASA websites.

b. Ensure the NASA Web Privacy Policy is posted (or linked to) on official NASA websites and applications hosted on third-party websites and applications.

c. Make the NASA Web Privacy Policy available through the NASA website.

d. Ensure that the NASA Web Privacy Policy is translated into a standardized machine-readable format.

5.6.2.2 The SAOP shall:

a. Ensure the NASA Web Privacy Policy:

(1) Includes description of the information being collected.

(2) Includes the purpose for the collection.

(3) Includes the official use of, or need for, the collected information.

(4) Specifies what information NASA collects automatically (e.g., user's internet protocol (IP) address, location, and time of visit) and identifies the use for which it is collected (e.g., site management or security purposes).

(5) Informs visitors as to whether their provision of the requested information is voluntary.

(6) Informs visitors on how to grant consent for the use of voluntarily provided information.

(7) Informs visitors on how to grant consent for NASA to utilize the information that the website collects for a use other than statutorily mandated or authorized routine uses under the Privacy Act.

(8) Notifies visitors of their rights under the Privacy Act for SOR.

(9) Incorporates information to meet the requirements of 15 U.S.C. §§ 6501-6506, where needed.

(10) Includes information on the redress mechanism.

(11) Notifies visitors as to how the Agency handles unsolicited e-mail, including the fact that the sender's privacy is not guaranteed.

b. Disclose, in the applicable NASA Web Privacy Policy, a third party's involvement in Agency applications when they are embedded within a NASA website.

5.6.2.3 The Center CIO shall:

a. Examine and monitor the third party's privacy policy when the Center uses a third-party website or application to evaluate risk and determine whether its use is acceptable to NASA.

b. Ensure the NASA Web Privacy Policy is incorporated into all Center public-facing NASA websites.

5.6.2.4 The CPO shall:

a. Review the NASA Web Privacy Policy to ensure compliance with this NPR and Federal requirements.

b. Recommend updates to the NASA Web Privacy Policy when needed.

5.6.2.5 The CPM shall assist the Center CIO in ensuring the NASA Web Privacy Policy is incorporated into all Center public facing NASA websites.

5.6.2.6 The ISO shall:

a. Ensure that privacy policies clearly and concisely inform visitors of the collection of PII.

b. Ensure that Privacy Act notification is provided to anyone entering an information system containing Privacy Act records.

c. Incorporate the NASA Web Privacy Policy into public-facing NASA websites.

5.7 Web Measurement and Customization Technology Use and Notice

5.7.1 Overview

5.7.1.1 Web measurement and customization technologies are used "... to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience" per OMB M-10-22. The use of this technology is permitted to improve NASA's online services; however, the use and notice requirements as outlined by OMB and NASA requirements are to be first be satisfied.

5.7.1.2 Specific information on when and how these technologies may be used at NASA is detailed in ITS-HBK-1382.06-01.

5.7.2 Procedural Requirements

5.7.2.1 The SAOP shall:

a. Ensure the NASA Privacy Policy describes the use of third-party websites and applications, as outlined by OMB.

b. Evaluate and approve or disapprove waivers for Web Measurement and Customization Technology that collects PII prior to use of that technology, as defined in ITS-HBK-1382.06, and annually thereafter.

5.7.2.2 The Center CIO shall approve any multi-session Web Measurement and Customization Technology prior to use when no PII is collected as defined in ITS-HBK-1382.06-01, and annually thereafter.

5.7.2.3 The NASA CPO shall advise the SAOP on web measurement and customization technology use at NASA.

5.7.2.4 The CPM shall advise the ISO on web measurement and customization technology use and requirements.

5.7.2.5 The ISO shall:

a. Ensure Web Measurement and Customization Technology use is compliant with requirements outlined in ITS-HBK-1382.06-01.

b. Ensure that the website utilizing approved Web Measurement and Customization Technology provides clear and conspicuous notice concerning the use of the technology and includes:

(1) The nature of the information collected.

(2) The purpose and use of the information.

(3) Whether, and to whom, the information will be disclosed.

(4) What privacy safeguards are applied to the information collected.

(5) Consequences to the visitor, or NASA user, of opting out.

c. Seek a waiver from the SAOP to use Web Measurement and Customization Technology when required, as described in ITS-HBK-1382.06-01.

Chapter 6 Protect

6.1 Overview

6.1.1 The Protect chapter describes NASA's data processing safeguards and incident response plans and procedures.

6.1.2 Data processing safeguards are deeply intertwined with information security requirements, as nearly all privacy-related information will be stored on or processed by some manner of information system. Readers are directed to consult NPR 2810.1, which governs NASA information security requirements, for further information on NASA cybersecurity polices and risk management.

6.2 Privacy and Information Security

6.2.1 Overview

6.2.1.1 The Privacy and Information Security section describes NASA's initiatives for privacy and information security. This section addresses requirements that all NASA PII will be secured, as directed by the Privacy Act; 44 U.S.C. § 3601; OMB M-06-15, OMB M-06-19, OMB M-07-16; and NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

6.2.1.2 NASA has a responsibility to protect the confidentiality, integrity, and availability of NASA information and information systems. The categorization of information systems may be Low, Moderate, or High as defined in NIST SP 800-60 Rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories and Federal Information Processing Standard Publications (FIPS PUB) 199. Information systems containing PII or aggregated contact information for NASA employees or contractors, such as a directory service, are categorized at a minimum Confidentiality level of Moderate.

6.2.1.3 All PII is to be handled and protected as CUI in accordance with NPR 2810.7.

6.2.1.4 NASA Privacy and Information Security procedures are governed by ITS-HBK-1382.04, Privacy and Information Security Overview.

6.2.2 Procedural Requirements

6.2.2.1 The SAOP shall implement privacy policies and procedures to ensure the confidentiality and integrity of privacy information.

6.2.2.2 The Center CISO, jointly with the CPM, shall ensure that the protection of privacy information is maintained throughout the creation, transmission, storage, use, and disposition of information.

6.2.2.3 The CPM, jointly with the Center CISO, shall ensure that the protection of privacy information is maintained throughout the creation, transmittal, storage, use, and disposition of information.

6.2.2.4 The ISO and User supervisors shall:

a. Ensure that access to PII is limited to those NASA users who have a need for access.

b. Ensure the protection of PII from unauthorized access or disclosure throughout its life cycle.

c. Ensure development and documentation of administrative, technical, and physical safeguards that protect against any anticipated threats or hazards to the security or integrity of records and against the potential of their unauthorized use in accordance with the requirements outlined in NPR 2810.1 and NPR 2810.7.

d. Ensure all computer-readable data extracts from databases containing PII are logged and verified, including information on whether the extracted data have been erased within 90 days or that the data's use is still required.

e. Ensure PII is encrypted on any mobile medium (e.g., e-mail, memory stick, CD/DVD, etc.), at rest, and that other security controls are in place to render PII unusable by unauthorized individuals.

f. Ensure all required security controls are implemented and maintained.

6.2.2.5 The NASA User shall:

a. Limit disclosure of information on individuals from a SOR only in accordance with 14 CFR pt. 1212 routine uses of the Privacy Act records published in the applicable SORN.

b. Request Privacy Act records only under appropriate authority.

c. Ensure that any PII on mobile devices is safeguarded, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards and NIST guidance, and in accordance with NPR 1600.1, NASA Security Program Procedural Requirements for sensitive information.

d. Ensure that PII is protected during transmission, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards, NIST guidance, and in accordance with NPR 1600.1.

e. Ensure that all PII transmitted or downloaded, in any format or media, to or from mobile devices is properly encrypted according to NPR 1600.1.

f. Label any mobile device or portable media containing PII in accordance with NPR 1600.1.

g. Remove PII from Agency premises or download and store PII remotely only under conditions prescribed in NPR 2810.7.

h. Ensure the proper disposition and/or sanitization of files, records, and/or media containing privacy information in accordance with the standards outlined in ITS-HBK-2810.11-02, Media Protection: Digital Media and Sanitization.

6.3 Privacy Incident Response and Management

6.3.1 Overview

6.3.1.1 The Privacy Incident Response and Management section describes NASA's response to incidents involving the breach of PII entrusted to NASA's custody or managed by a contractor on NASA's behalf. This section addresses breach response requirements within OMB M-06-19, and

OMB M-07-16.

6.3.1.2 The mechanism for response to a confirmed moderate or high-risk breach is a privacy BRT which is convened within 24 hours of the incident in accordance with ITS-HBK-1382.05, Privacy Incident Response: Breach Response Team Checklist and Management. In such a case, a Center BRT is convened when a breach of sensitive PII meets the threshold outlined in the handbooks associated with this directive. The BRT analyzes risk of identity theft in accordance with OMB requirements and NASA policies and guidelines, prepares recommendations for remediation and notification plans, drafts breach notification letters, determines the mechanism of public notice, assists the ISO in preparing Frequently Asked Questions (FAQs), notifies and continues to provide updates to the NASA CPO on the status of the breach and any related breach response activities, and submits findings and recommendations to the SAOP for approval.

6.3.1.3 Non-governmental PII that is the property of the custodian, or entrusted to that person by friends or family, or a NASA contractor, grantee, etc., including corporate data used for non-governmental purposes but stored on NASA equipment is not covered by this NPR. While the limited personal use of government equipment may be permitted by NID 2540.138, NASA has no responsibility for the loss or compromise of such information.

6.3.1.4 NASA privacy breach response procedures are governed by ITS-HBK 1382.05, and ITS-HBK-2810.09, Incident Response and Management.

6.3.2 Procedural Requirements

6.3.2.1 The SAOP shall:

a. Establish, implement, and publish Agency PII breach response and management policies and procedures in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

b. Review, approve, or amend BRT recommended actions and notification plans.

c. Advise NASA senior management on sensitive PII breaches and remediation progress.

d. Activate an Agency BRT if the situation warrants a NASA-wide activation.

e. Advise NASA senior management when notification and action plans need to be executed at a NASA-wide level.

f. Ensure that all NASA users receive incident reporting training as outlined in Chapter 3 of this NPR.

6.3.2.2 The Center CIO shall advise the BRT when needed.

6.3.2.3 The NASA CPO shall:

a. Assist the SAOP in fulfilling PII breach responsibilities.

b. Recommend to the SAOP to activate an Agency BRT when needed if such BRT is not already activated.

c. Maintain coordination and communication with the SAISO and the NASA SOC for incident reporting, tracking, and closure of sensitive PII breaches.

d. Provide overall direction to an Agency BRT for sensitive PII breaches.

e. Provide overall breach response guidance for sensitive PII BRT activities.

f. Update the SAOP on the status of the breach and breach response activities.

g. Submit, when needed, BRT findings and recommendations to the NASA SAOP for approval.

6.3.2.4 The CPM shall:

a. Ensure suspected loss, actual loss, and unauthorized access to PII are reported in accordance with NASA policy and procedures stated in ITS-HBK 1382.05-01.

b. Function as a core Center BRT member advising the BRT on privacy related policy, requirements, and procedures.

c. Ensure that the steps outlined in handbook-level guidance are met.

d. Participate in suspected PII breach initial investigations, determinations, reporting, and response efforts.

e. Produce reports and close out breach actions, as required.

f. Ensure necessary follow-up actions on remediation efforts, in coordination with the Center CISO, are conducted to reduce risk of repeat offenses.

6.3.2.5 The ISO shall:

a. Advise the BRT on the specifics of the affected information system(s) and/or information.

b. Advise on policies, processes, and impacts related to the breach.

c. Support recommendations from the BRT.

6.3.2.6 The NASA User shall report any suspected or confirmed breach of any form of PII as an Information Security incident to the NASA SOC immediately upon discovery.

6.3.2.7 The OIG shall investigate PII breaches involving suspected criminal intent and coordinate with the BRT on such matters.

6.3.2.8 The Office of the General Counsel (OGC) shall advise all BRTs on legal issues and review for legal sufficiency all proposed notification materials.

6.3.2.9 The Center Chief Counsel shall advise the Center BRT on legal issues and review for legal sufficiency proposed notification materials.

6.3.2.10 The Center Office of Communications (or equivalent office) may:

a. Advise on and review proposed notification materials and approaches.

b. Generate releases and other public notifications as requested.

6.3.2.11 The CO/COR, in situations where the breach involves information maintained on NASA's behalf by or on contractors, shall serve as the interface between the Government and contracted parties.

6.3.2.12 The Center Human Resources Director may designate a Human Resources staff member to

serve as a member of the BRT. The designated staff member will participate in gathering and documenting information and evidence about the role of any civil servant employee in the breach.

6.3.2.13 The Center Human Resources Employee Relations Specialists may advise the civil servants' supervisor(s) on corrective action, which may include formal or informal disciplinary action.

Appendix A. Definitions

Information in Identifiable Form (IIF). In Section 208(d) of 44 U.S.C. § 3601, IIF is defined as "... any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

In accordance with OMB M-03-22, IIF "... is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, (i.e., indirect identification). (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

Refer to ITS-HBK-1382.03-01for additional information on IIF.

NASA User. Any explicitly authorized patron of a NASA information system.

Non-Sensitive Personally Identifiable Information (PII). Non-Sensitive PII is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

Member of the Public. Refer to ITS-HBK-1382.03-01for the distinction of member of the public as it pertains to 44 U.S.C. § 3604 and 44 U.S.C. § 3501.

Personally Identifiable Information (PII). OMB M-07-16, PII "... refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

In accordance with OMB M-10-23, "... [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."

For purposes of NASA policy, sensitive PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes, as allowed under NID 2540.138. Examples of such excluded data include contact information for family, relatives, and doctors.

Refer to ITS-HBK-1382.03-01for additional information on PII.

Privacy Act Information. Information that is maintained in a "system of records," which the Act defines as a group of agency-controlled records from which information is retrieved by a unique identifier, such as an individual's name, date of birth, social security number, or employee identification number.

Privacy Act Record. A record that is part of a Privacy Act System of Records.

Privacy Act System of Records (SOR). A group of records from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned to that individual.

Privacy Breach. A privacy breach is also known as an "incident." An incident is any adverse event or situation associated with any information collection containing PII that poses a threat to integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information. Refer to ITS-HBK-1382.05 for specific information on privacy breach.

Privacy Impact Assessment (PIA). In accordance with OMB M-03-22, a PIA "... is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

Refer to ITS-HBK-1382.03-01for additional information on PIAs.

Record. The Privacy Act defines a "record" as any individually identifiable set of information that an agency might maintain about a person. Such records may include a wide variety of personal information including, but not limited to, information about education, financial transactions, medical history, criminal history, or employment history.

Sensitive Personally Identifiable Information. This definition is related to incident reporting only as outlined in this NPR. All PII, regardless of whether it is sensitive or non-sensitive, is required to be protected as outlined in this NPR and as defined in OMB M-07-16.

Sensitive PII is a combination of PII elements, which if lost, compromised, or disclosed without authorization could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Refer to ITS-HBK-1382.03-01 for additional information on the distinction of sensitive versus non-sensitive PII.

Appendix B. Acronyms

BRT	Breach Response Team
CFR	Code of Federal Regulation
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CO	Contracting Officer
COPPA	Children's Online Privacy Protection Act
COR	Contracting Officer Representative
CPM	Center Privacy Manager
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DO	Data Owner
DVD	Digital Versatile Disc
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GOCO	Government Owned, Contractor Operated
IIF	Information in Identifiable Form
IO	Information Owner
IP	Internet Protocol
ISO	Information System Owner
ITSATC	Information Technology Security Awareness and Training Center
ITS-HBK	Information Technology Security Handbook
JPL	Jet Propulsion Laboratory
MPII	Master Privacy Information Inventory
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology

NITR	NASA Interim Technical Requirement
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAI	Privacy Act Information
PAO	Privacy Act Officer
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL-[number]	Planning
P.L.	Public law
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SOC	Security Operations Center
SOR	System of Records
SORN	System of Records Notice
SP	[NIST] Special Publication
SSN	Social Security Number
U.S.C.	United States Code

Appendix C. Requirements Matrices

C.1 Administrator

Para #	Requirement
1.2.2.1a	Ensure the protection of PII within NASA's information and information systems.
1.2.2.1b	Assign a SAOP, who maintains the Agency's privacy program and its overall objectives and priorities.
4.2.2.1	The Administrator shall ensure, in accordance with Social Security Number Fraud Prevention Act of 2017, Pub. L. 115-59, 131 Stat. 1152 (2017), NASA does not include a social security number (SSN) on any NASA-developed document sent by physical mail unless: a. The Administrator approves such inclusion; and b. Inclusion is necessary because: (1) Inclusion is required by law or regulation. (2) An SSN is needed to identify a specific individual and no other substitute is available. (3) Inclusion is needed to fulfill a compelling Agency business need.

C.2 Agreement Managers

Para #	Requirement
1.2.2.11	Contracting Officers (COs) or Agreement Managers shall ensure that the requirements of this directive are included and in scope for all NASA contracts, Space Act agreements, cooperative agreements, partnership agreements, or other agreements pursuant to which privacy information (e.g., PII, PHI, PAI) is being collected, processed, stored, or transmitted.

C.3 Center Breach Response Team Members

Para #	Requirement
3.2.2.6	The Center Breach Response Team (BRT) members shall participate in annual BRT training and exercises.

C.4 Center Chief Counsel

Para #	Requirement

6.3.2.9	The Center Chief Counsel shall advise the Center BRT on legal issues and review for legal sufficiency proposed notification materials.

C.5 Center Chief Information Officer

Para #	Requirement
1.2.2.8a	Ensure that all Center information and information systems comply with the provisions of this NPR.
1.2.2.8b	Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy.
1.2.2.8c	Support the CPM in protecting PII and/or Information in Identifiable Form (IIF) at the Center.
1.2.2.8d	Ensure that Information Owners (IOs), Information System Owners (ISOs), and Data Owners (DOs) assess the privacy aspects of information collections and information systems for which they are responsible and ensure all required security safeguards are implemented in accordance with current NASA policy and procedural requirements for the collection, use, maintenance, and dissemination of personal information.
5.6.2.3a	Examine and monitor the third party's privacy policy when the Center uses a third-party website or application to evaluate risk and determine whether its use is acceptable to NASA.
5.6.2.3b	Ensure the NASA Web Privacy Policy is incorporated into all Center public-facing NASA websites.
5.7.2.2	The Center CIO shall approve any multi-session Web Measurement and Customization Technology prior to use when no PII is collected as defined in ITS-HBK-1382.06-01, and annually thereafter.
6.3.2.2	The Center CIO shall advise the BRT when needed.

C.6 Center Chief Information Security Officer

Para #	Requirement
1.2.2.9	The Center Chief Information Security Officer (CISO) shall support the CPM in protecting PII at the Center.
6.2.2.2	The Center CISO, jointly with the CPM, shall ensure that the protection of privacy information is maintained throughout the creation, transmission, storage, use, and disposition of information.

C.7 Center Human Resources Employee Relations Specialist

Para #	Requirement
6.3.2.13	The Center Human Resources Employee Relations Specialists may advise the civil servants' supervisor(s) on corrective action, which may include formal or informal disciplinary action.

C.8 Center Human Resources Director

Para #	Requirement
6.3.2.12	The Center Human Resources Director may designate a Human Resources staff member to serve as a member of the BRT. The designated staff member will participate in gathering and documenting information and evidence about the role of any civil servant employee in the breach.

C.9 Center Office of Communications (or equivalent office)

Para #	Requirement
6.3.2.10	The Center Office of Communications (or equivalent office) may: a. Advise on, and review, proposed notification materials and approaches. b. Generate releases and other public notifications as requested.

C.10 Center/Executive Director

Para #	Requirement
1.2.2.7a	Appoint a Center Privacy Manager (CPM).
1.2.2.7b	Support the protection and management of PII at the Center and consult with the CPM on matters pertaining to privacy.

C.11 Chief Information Officer

Para #	Requirement
1.2.2.2a	Provide guidance to the SAOP.
1.2.2.2b	Update NPD 1382.17, NASA Privacy Policy, to ensure NASA is current with changes in Federal privacy policy.

5.6.2.1a	Ensure the NASA Web Privacy Policy is posted (or linked to) all public facing NASA websites.
5.6.2.1b	Ensure the NASA Web Privacy Policy is posted (or linked to) on official NASA websites and applications hosted on third-party websites and applications.
5.6.2.1c	Make the NASA Web Privacy Policy available through the NASA website.
5.6.2.1d	Ensure that the NASA Web Privacy Policy is translated into a standardized machine-readable format.

C.12 Contracting Officer Representatives

Para #	Requirement
6.3.2.11	The CO/COR, in situations where the breach involves information maintained on NASA's behalf by or on contractors, shall serve as the interface between the Government and contracted parties.

C.13 Contracting Officers

Para #	Requirement
1.2.2.11	Contracting Officers (COs) or Agreement Managers shall ensure that the requirements of this directive are included and in scope for all NASA contracts, Space Act agreements, cooperative agreements, partnership agreements, or other agreements pursuant to which privacy information (e.g., PII, PHI, PAI) is being collected, processed, stored, or transmitted.
6.3.2.11	The CO/COR, in situations where the breach involves information maintained on NASA's behalf by or on contractors, shall serve as the interface between the Government and contracted parties.

C.14 Center Privacy Manager

Para #	Requirement
1.2.2.10a	Serve as the Center advisor to the Center Director, Center CIO, Center CISO, and Information System Owners (ISOs) on all matters pertaining to privacy.
1.2.2.10b	Function as the primary Center point of contact/liaison to the NASA CPO and NASA PAO.
1.2.2.10c	Work with ISOs to review and aid in ensuring compliance with all privacy requirements, as needed.

1.2.2.10d	Validate the proper disposition and/or sanitization process for files and records (paper, electronic, or other media formats), which contain privacy information.
1.2.2.10e	Ensure the NASA privacy program is implemented at the Center in accordance with NASA policy.
1.2.2.10f	Ensure that IOs, ISOs, and DOs perform the required information collection assessments (i.e., PTAs and PIAs) and aid in the development of any additional documentation indicated as required upon completion of the PTA (or PIA if required). (This includes SORNs, Privacy Act Federal Register notices, and Privacy Act Statements.)
1.2.2.10g	Serve as their Center's liaison for the controlled unclassified information (CUI) program unless a different liaison is identified by the Center's leadership.
2.2.2.2	The CPM shall ensure the MPII established per Section 2.2.1.1a accurately reflects all electronic and non-electronic collections of information for their respective Center and is current.
2.3.2.3a	Assist ISOs in the completion of PTAs and, when needed, PIAs.
2.3.2.3b	Conduct timely reviews of applications and information systems, including websites, PTAs and PIAs to ensure the ISO has addressed adequate protection of privacy and/or Privacy Act information (PAI).
2.3.2.3c	Ensure the ISOs update PTAs and, when needed, PIAs.
2.3.2.3d	Conduct annual PIA reviews.
2.3.2.3e	Ensure procedures exists to dispose of data at the Center level according to NRRS 1441.1, NPR 2810.1, and NPR 2810.7.
3.2.2.3a	Complete privacy role-based training, as required.
3.2.2.3b	Ensure awareness and training programs are conducted at the Center level.
3.3.2.4a	Update the NASA CPO, Center CIO, and Center CISO on the status of meeting the privacy requirements at the Center.
3.3.2.4b	Respond to various privacy related mandates and requests for information from the NASA CPO and NASA PAO.
3.3.2.4c	Report any Privacy (PII) or Privacy Act violations to the CPO.
3.3.2.4d	Track planned, in progress, and completed corrective actions taken to remedy deficiencies identified in compliance reviews.
3.3.2.4e	Ensure the NASA MPII is up to date and accurately reflects all electronic and non-electronic collections of information for their respective Center.
3.3.2.4f	Report all significant privacy related activities (e.g., BRT activities and privacy complaints) to the CPO.

3.3.3.5a	Coordinate 44 U.S.C. § 3551 privacy reporting data collection efforts for their Center and report to the NASA CPO, Center CIO, and Center CISO.
3.3.3.5b	Coordinate Privacy Act reviews as directed by the NASA PAO.
3.4.2.3a	Receive and seek to address Center-level privacy complaints.
3.4.2.3b	Report Center-level privacy complaints to the NASA CPO via the process defined in ITS-HBK-1382.06-01.
3.5.2.3	The CPM shall provide support to the CPO to ensure adherence to the requirements of this NPR at the Center level.
3.6.2.4	The CPM shall forward any Privacy Act record access requests received to the relevant System Manager for processing in accordance with 14 CFR pt. 1212.
4.2.2.4a	Work with ISOs to ensure that all PII is maintained with accuracy, relevance, timeliness, and completeness.
4.2.2.4b	Coordinate annual review activities at the Center level with ISOs to ensure PII is collected in accordance with this policy and to reduce or eliminate unnecessary collections of PII.
4.2.2.4c	Work with ISOs to eliminate the unnecessary use of SSNs.
5.4.2.3	The CPM shall work with ISOs and the PAO to ensure the Privacy Act Statement meets the requirements of the Privacy Act.
5.5.2.3a	Work with ISOs in identifying the need for a Privacy Act SORN.
5.5.2.3b	Assist the ISO in drafting a SORN for publication in the Federal Register, if not already covered under an existing SORN.
5.5.2.3c	Provide the NASA PAO with draft SORNs, as required.
5.5.2.3d	Conduct SORN reviews, as required.
5.5.2.3e	Coordinate the review and approval of new draft SORNs and Privacy Act notice updates with ISOs and the NASA PAO.
5.6.2.5	The CPM shall assist the Center CIO in ensuring the NASA Web Privacy Policy is incorporated into all Center public facing NASA websites.
5.7.2.4	The CPM shall advise the ISO on Web Measurement and Customization Technology use and requirements.
6.2.2.3	The CPM, jointly with the Center CISO, shall ensure that the protection of privacy information is maintained throughout the creation, transmittal, storage, use, and disposition of information.
6.3.2.4a	Ensure suspected loss, actual loss, and unauthorized access to PII are reported in accordance with NASA policy and procedures stated in ITS-HBK 1382.05-01.

6.3.2.4b	Function as a core Center BRT member advising the BRT on privacy related policy, requirements, and procedures.
6.3.2.4c	Ensure that the steps outlined in handbook-level guidance are met.
6.3.2.4d	Participate in suspected PII breach initial investigations, determinations, reporting, and response efforts.
6.3.2.4e	Produce reports and close out breach actions, as required.
6.3.2.4f	Ensure necessary follow-up actions on remediation efforts, in coordination with the Center CISO, are conducted to reduce risk of repeat offenses.

C.15 Chief Privacy Officer

Para #	Requirement
1.2.2.5a	Oversee and manage the development and implementation of policy and procedure, guidance, directives, and requirements for NASA in support of compliance with Federal laws, statutes, and Government-wide policy as directed by the SAOP.
1.2.2.5b	Ensure that NASA complies with privacy requirements within Federal statutes listed in this directive, including the collection, maintenance, use, and dissemination of privacy information.
1.2.2.5c	Develop and maintain NASA privacy policies, procedural requirements, and handbooks as directed by the SAOP.
1.2.2.5d	Establish Agency requirements and processes for conducting PTAs and PIAs for new or significantly changed applications, websites, or information systems, and make PIAs publicly available (unless public release is otherwise prohibited).
1.2.2.5e	Oversee and provide guidance in the implementation and the day-to-day operation of the NASA-wide privacy program as directed by the SAOP.
1.2.2.5f	Review NASA's compliance with information privacy laws, regulations, and policies annually to validate effectiveness and ensure conformity with current Federal policies and guidance as directed by the SAOP.
2.3.2.2a	Implement Agency policy, requirements, and processes for conducting PTAs and PIAs, for new or revised applications and information systems.
2.3.2.2b	Ensure PIAs are thorough and meet all applicable standards.
2.3.2.2c	Ensure that completed PIAs are made publicly available for applications and information systems, including websites, which collect and/or maintain IIF on members of the public, consistent with Federal policy, unless otherwise prohibited.
3.2.2.2a	Review and approve all privacy awareness and training materials.
3.2.2.2b	Develop privacy awareness and training materials.

3.2.2.2c	Work with the Information Technology Security Awareness and Training Center (ITSATC) to ensure privacy awareness and training materials meet information security training requirements.
3.2.2.2d	Ensure the privacy training: (1) For the NASA user explains the policies and procedures for safeguarding PII collected and maintained at NASA. (2) For the NASA user explains the privacy rules of behavior and consequences. (3) For the NASA user with access to NASA data, explains that willful disclosure of information to individuals not entitled to Privacy Act records or sensitive privacy information in any form is strictly prohibited. (4) For persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record within any SOR, explains the requirements regarding the protection, use, and release of the Privacy Act records. (5) For persons involved in the design, development, operation, or maintenance of any PII collection, explains the requirements regarding the protection, use, and release of the records.
3.2.2.2e	Determine the annual training requirements for CPMs.
3.3.2.3	The NASA CPO shall update the SAOP on privacy metrics annually as part of the 44 U.S.C. § 3551 reporting process.
3.3.3.3a	Produce and provide NASA's privacy reports required by OMB and 44 U.S.C. § 3551 to the NASA SAISO and the NASA SAOP.
3.3.3.3b	Ensure that privacy reviews are conducted in accordance with the schedule outlined in ITS-HBK-1382.08.
3.4.2.2	The NASA CPO shall work with the SAOP to record, track, and address privacy complaints.
3.5.2.2a	Advise the SAOP on consequences for violating this NPR.
3.5.2.2b	Advise the CPM on consequences for violating this NPR at the Center level.
3.5.2.2c	Establish requirements and procedures for reporting known, suspected, or likely violations of the privacy requirements of this NPR.
3.6.2.2	The NASA CPO shall assist the SAOP in redressing PII issues.
3.8.2.2	The CPO shall work with the SAOP and the SAISO to ensure that privacy risk is incorporated into NASA’s overall risk management strategies.
4.2.2.3	The NASA CPO shall coordinate and direct annual NASA-wide review activities to reduce or eliminate unnecessary collections of PII.
5.3.2.1	The CPO shall maintain Agency guidance for compliance with 15 U.S.C. §§ 6501-6506.

5.6.2.4a	Review the NASA Web Privacy Policy to ensure compliance with this NPR and Federal requirements.
5.6.2.4b	Recommend updates to the NASA Web Privacy Policy when needed.
5.7.2.3	The NASA CPO shall advise the SAOP on Web Measurement and Customization Technology use at NASA.
6.3.2.3a	Assist the SAOP in fulfilling PII breach responsibilities.
6.3.2.3b	Recommend to the SAOP to activate an Agency BRT when needed if such BRT is not already activated.
6.3.2.3c	Maintain coordination and communication with the SAISO and the NASA SOC for incident reporting, tracking, and closure of sensitive PII breaches.
6.3.2.3d	Provide overall direction to an Agency BRT for sensitive PII breaches.
6.3.2.3e	Provide overall breach response guidance for sensitive PII BRT activities.
6.3.2.3f	Update the SAOP on the status of the breach and breach response activities.
6.3.2.3g	Submit, when needed, BRT findings and recommendations to the NASA SAOP for approval.

C.16 Freedom of Information Act Officer

Para #	Requirement
3.6.2.6	The Freedom of Information Act (FOIA) Officer shall process Privacy Act record access requests the Officer receives from an individual seeking access to the individual's NASA maintained record in accordance with 14 CFR pt. 1212 and the Privacy Act in conjunction with the System Manager.

C.17 Information Owner

Para #	Requirement
3.6.2.5	The System Manager (the ISO or IO) shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 CFR pt. 1212 and the Privacy Act.

C.18 Information System Owner

Para #	Requirement

1.2.2.12a	Acquire, develop, integrate, operate, modify, maintain, and dispose of information systems containing PII in a manner consistent with Federal statutes, regulation, and NASA privacy policies.
1.2.2.12b	Ensure compliance with the Privacy Act for applications and information systems containing Privacy Act records.
1.2.2.12c	Verify with the CO/Contracting Officer Representative (COR) that any contract that requires the operation of a System of Records (SOR) on behalf of NASA includes the clauses required per Federal Acquisition Regulations, 48 CFR pt. 24.
1.2.2.12d	Notify the CO when purchase requests include services covered by the Privacy Act or Paperwork Reduction Act (44 U.S.C. § 3501), 44 U.S.C. § 3501 et seq.
1.2.2.12e	Notify the CO when contractor services will require or include access to PII collected by or on behalf of NASA.
1.2.2.12f	Verify that the contract statement of work identifies this NPR as outlining the NASA-specific requirements to be followed by the contractor.
2.3.2.4a	Ensure that a PTA is conducted and approved for the applications and information systems, including websites, under their purview.
2.3.2.4b	Ensure that a PIA is reviewed and approved for: (1) An information system that collects, maintains, or disseminates IIF from or about members of the public; or (2) An electronic collection of IIF for ten or more individuals, consistent with 44 U.S.C. § 3501.
2.3.2.4c	Ensure that they conduct a re-evaluation of PTAs and, when needed, PIAs following significant modifications to all applications and information systems, including websites.
2.3.2.4d	Ensure that a PIA is conducted prior to use of a third-party website or application that collects PII.
2.3.2.4e	Review completed PTAs and PIAs annually to ensure ongoing accuracy.
3.2.2.4a	Ensure that all NASA users who have access to PII or who develop or supervise procedures for handling PII are trained and are compliant with policies and procedures in NPD 1382.17, this directive, and referenced documents for safeguarding PII collected and maintained at or on behalf of NASA.
3.2.2.4b	Ensure that persons involved in the design, development, operation, or maintenance of any Privacy Act SOR, or in the maintenance of any record in any SOR, are trained in the requirements regarding the protection, use, and release of the Privacy Act records.
3.2.2.4c	Ensure that persons involved in the design, development, operation, or maintenance of any PII collection are trained in the requirements regarding the protection, use, and release of the records.

3.3.2.5a	Report to the CPM on the status of compliance with NASA Privacy requirements through the PTA and PIA processes accomplished in RISCS.
3.3.2.5b	Control disclosures from their SOR and maintain accountings of all disclosures of information in accordance with Privacy Act NASA Regulations, 14 CFR pt. 1212.
3.4.2.4a	Receive and seek to address privacy complaints associated with the application, information system, or website.
3.4.2.4b	Report application, information system, or website privacy complaints to the CPM.
3.5.2.4a	Meet publication requirements for Privacy Act SOR. Any official who willfully maintains a Privacy Act SOR without meeting the publication requirements is subject to possible criminal penalties or administrative sanctions, or both.
3.5.2.4b	Be held accountable for privacy violations of this NPR; penalties range from criminal to administrative.
3.6.2.5	The System Manager (the ISO or IO) shall process Privacy Act record access requests from an individual seeking access to their individual NASA maintained record in accordance with 14 CFR pt. 1212 and the Privacy Act.
4.2.2.5a	Eliminate the collection of information if the information is unnecessary to a NASA program and/or its associated mission.
4.2.2.5b	Ensure that all privacy information is maintained with accuracy, relevance, timeliness, and completeness.
4.2.2.5c	Ensure that Privacy Act records are collected and maintained in accordance with NASA Privacy Act policies.
4.2.2.5d	Conduct annual review activities to reduce or eliminate unnecessary collections of PII.
4.2.2.5e	Avoid the collection of SSNs, in accordance with NPD 1382.17, unless required by statute or some another requirement mandating the use of SSNs.
5.2.2.3	The ISO shall work with the PAO to prepare and ensure publication of a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.
5.3.2.2a	Ensure compliance with 15 U.S.C. §§ 6501-6506 for websites intended to be used by, or targeted to, children under the age of 13 that collect PII.
5.3.2.2b	Ensure that notice is provided concerning what information is being collected from children by the operator, how the information will be used, and the operator’s disclosure practices.
5.3.2.2c	Ensure verifiable parental approval is obtained for the collection, use, or disclosure of information from children.

5.3.2.2d	Provide a process for parental review of information collected from the child.
5.3.2.2e	Provide an opportunity for parental refusal to permit the operator's future use of the information or future collection of information.
5.3.2.2f	Provide a means for the parent to obtain the personal information collected from the child.
5.4.2.4a	Ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are presented at the point of collection with a Privacy Act Statement that: (1) Is presented either on the information collection sheet or screen, or via a separate sheet or screen that the individuals can print and retain; (2) Complies with the requirements outlined in 14 CFR §1212.602; and (3) Is in a format that the individual may be able to retain in a physical or hard copy.
5.4.2.4b	Ensure that new NASA forms or Center forms created for the collection of SOR information provide the correct and specific Privacy Act Statement for that SOR.
5.5.2.4a	Limit the maintenance of Privacy Act records on individuals that are retrievable by name or other personal identifier to only those instances for which a Privacy Act SORN has been published in the Federal Register.
5.5.2.4b	Provide draft content to enable the PAO to complete a SORN for publication in the Federal Register, if not already covered under an existing SORN.
5.5.2.4c	Work with the CPM and the NASA PAO to publish a SORN in the Federal Register.
5.6.2.6a	Ensure that privacy policies clearly and concisely inform visitors of the collection of PII.
5.6.2.6b	Ensure that Privacy Act notification is provided to anyone entering an information system containing Privacy Act records.
5.6.2.6c	Incorporate the NASA Web Privacy Policy into public-facing NASA websites.
5.7.2.5a	Ensure Web Measurement and Customization Technology use is compliant with requirements outlined in ITS-HBK-1382.06-01.
5.7.2.5b	Ensure that the website utilizing approved Web Measurement and Customization Technology provides clear and conspicuous notice concerning the use of the technology and includes: (1) The nature of the information collected. (2) The purpose and use of the information. (3) Whether, and to whom, the information will be disclosed. (4) What privacy safeguards are applied to the information collected. (5) Consequences to the visitor, or NASA user, of opting out.

5.7.2.5c	Seek a waiver from the SAOP to use Web Measurement and Customization Technology when required, as described in ITS-HBK-1382.06-01.
6.2.2.4a	Ensure that access to PII is limited to those NASA users who have a need for access.
6.2.2.4b	Ensure the protection of PII from unauthorized access or disclosure throughout its life cycle.
6.2.2.4c	Ensure development and documentation of administrative, technical, and physical safeguards that protect against any anticipated threats or hazards to the security or integrity of records and against the potential of their unauthorized use in accordance with the requirements outlined in NPR 2810.1 and NPR 2810.7.
6.2.2.4d	Ensure all computer-readable data extracts from databases containing PII are logged and verified, including information on whether the extracted data have been erased within 90 days or that the data's use is still required.
6.2.2.4e	Ensure PII is encrypted on any mobile medium (e.g., e-mail, memory stick, CD/DVD, etc.), at rest, and that other security controls are in place to render PII unusable by unauthorized individuals.
6.2.2.4f	Ensure all required security controls are implemented and maintained.
6.3.2.5a	Advise the BRT on the specifics of the affected information system(s) and/or information.
6.3.2.5b	Advise on policies, processes, and impacts related to the breach.
6.3.2.5c	Support recommendations from the BRT.

C.19 NASA User

Para #	Requirement
1.2.2.13a	Comply with all Federal laws, statutes, Government-wide, and NASA privacy policies and procedures in this and the referenced documents.
1.2.2.13b	Protect all PII in the user's custody (whether virtual, electronic, actual, or otherwise) from unauthorized disclosure, use, modification, or destruction so that the confidentiality, integrity, and availability of the information are preserved.
3.2.2.5a	Participate in mandatory privacy training prior to gaining access to NASA information and information systems, and yearly thereafter.
3.2.2.5b	Participate in privacy role-based training, as required.
3.3.2.6	The NASA User shall report any suspected or confirmed unauthorized disclosures of PII in any form to the Security Operations Center (SOC) in accordance with Agency ITS incident reporting procedures.

3.5.2.5	The NASA User shall be held accountable for violations of this NPR and related handbooks. Penalties may include reprimand, suspension, removal, or other administrative action, fines, additional privacy training or other actions in accordance with applicable laws and Agency disciplinary policy.
3.5.2.6	NASA Users may: a. Be subject to written reprimand, suspension, removal, or other administrative action under the following situations: (1) Knowingly failing to implement and maintain information security controls required by this NPR for the protection of PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII. (2) Failing to report any known or suspected loss of control or unauthorized disclosure of PII. (3) For managers, failing to adequately instruct, train, or supervise employees in their privacy responsibilities.
3.5.2.6b	Be subject to criminal penalties for willful and intentional violations of the Privacy Act.
4.2.2.6a	Not include an SSN on any NASA-developed document sent by physical mail unless the Administrator approves such inclusion in accordance with Section 4.2.2.1 of this directive. The process for gaining Administrator approval is governed by the CPO and detailed in ITS-HBK 1382.03-02, Privacy Annual Reporting Procedures: Reviewing and Reducing PII and Unnecessary Use of SSN.
4.2.2.6b	Ensure, if ever including an SSN on a NASA-developed document sent by physical mail in accordance with Section 4.2.2.6a of this directive: (1) Where feasible, the SSN is partially redacted; and (2) The SSN is not visible on the outside of any such package.
6.2.2.5a	Limit disclosure of information on individuals from a SOR only in accordance with 14 CFR pt. 1212 routine uses of the Privacy Act records published in the applicable SORN.
6.2.2.5b	Request Privacy Act records only under appropriate authority.
6.2.2.5c	Ensure that any PII on mobile devices is safeguarded, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards and NIST guidance, and in accordance with current NASA Security Program Procedural Requirements for sensitive information.
6.2.2.5d	Ensure that PII is protected during transmission, at a minimum, using encryption solutions which are compliant with Federal encryption algorithm standards, NIST guidance, and in accordance with NPR 1600.1, NASA Security Program Procedural Requirements for sensitive information.
6.2.2.5e	Ensure that all PII transmitted or downloaded, in any format or media, to or from mobile devices is properly encrypted according to NASA Security Program Procedural Requirements for sensitive information.

6.2.2.5f	Label any mobile device or portable media containing PII in accordance with current NASA Security Program Procedural Requirements for sensitive information.
6.2.2.5g	Remove PII from Agency premises or download and store PII remotely only under conditions prescribed in NPR 2810.7.
6.2.2.5h	Ensure the proper disposition and/or sanitization of files, records, and/or media containing privacy information in accordance with the standards outlined in ITS-HBK-2810.11-02, Media Protection: Digital Media and Sanitization.
6.3.2.6	The NASA User shall report any suspected or confirmed breach of any form of PII as an Information Security incident to the NASA SOC immediately upon discovery.

C.20 NASA User Supervisors

Para #	Requirement
6.2.2.4a	Ensure that access to PII is limited to those NASA users who have a need for access.
6.2.2.4b	Ensure the protection of PII from unauthorized access or disclosure throughout its life cycle.
6.2.2.4c	Ensure development and documentation of administrative, technical, and physical safeguards that protect against any anticipated threats or hazards to the security or integrity of records and against the potential of their unauthorized use in accordance with the requirements outlined in NPR 2810.1 and NPR 2810.7.
6.2.2.4d	Ensure all computer-readable data extracts from databases containing PII are logged and verified, including information on whether the extracted data have been erased within 90 days or that the data's use is still required.
6.2.2.4e	Ensure PII is encrypted on any mobile medium (e.g., e-mail, memory stick, CD/DVD, etc.), at rest, and that other security controls are in place to render PII unusable by unauthorized individuals.
6.2.2.4f	Ensure all required security controls are implemented and maintained.

C.21 Office of the General Counsel

Para #	Requirement
6.3.2.8	The OGC shall advise all BRTs on legal issues and review for legal sufficiency all proposed notification materials.

C.22 Office of Inspector General

Para #	Requirement
6.3.2.7	The OIG shall investigate PII breaches involving suspected criminal intent and coordinate with the BRT on such matters.

C.23 Privacy Act Officer

Para #	Requirement
1.2.2.6a	Ensure compliance with requirements of the Privacy Act.
1.2.2.6b	Oversee, manage, and implement the Privacy Act requirements for NASA.
3.3.3.4	The NASA PAO shall coordinate and conduct Privacy Act and OMB Circular A-130 reviews in accordance with the schedule outlined in ITS-HBK-1382.08-01.
3.6.2.3	The PAO shall provide a Privacy Act record access request process for individuals seeking access to their individual NASA maintained record in 14 CFR pt. 1212.
5.2.2.2	The NASA PAO shall work with the ISO to prepare and publish a notice in the Federal Register at least 30 days in advance of the establishment or revision of a matching program.
5.4.2.2	The NASA PAO shall work with the CPM to ensure the Privacy Act Statement meets the requirements of the Privacy Act.
5.5.2.2a	Review and revise draft SORNs in cooperation with the system manager.
5.5.2.2b	Coordinate the Agency and OMB reviews of SORNs and obtain SAOP signature for SORN submission to the Federal Register for publication through the NASA Federal Register Liaison Officer.
5.5.2.2c	Coordinate with CPMs in determining whether an existing NASA or other government SORN covers Privacy Act records maintained by NASA.

C.24 Senior Agency Information Security Officer

Para #	Requirement
1.2.2.4	The Senior Agency Information Security Officer (SAISO) shall provide necessary management and resources in support of the NASA-wide privacy program as established by the SAOP.

3.8.2.1	The SAISO shall ensure the Cybersecurity Risk Management Strategy required by NPR 2810.1, includes consideration of privacy risks within the context of the strategy.

C.25 Senior Agency Official for Privacy

Para #	Requirement
1.2.2.3a	Provide overall responsibility and accountability for ensuring NASA's implementation of privacy information protections.
1.2.2.3b	Ensure that NASA is compliant with applicable Federal laws, regulations, policies, guidelines, and NASA privacy program requirements.
1.2.2.3c	Develop and maintain a NASA-wide privacy program.
1.2.2.3d	Develop, maintain, and monitor NASA privacy goals and objectives.
1.2.2.3e	Approve handbooks related to this NPR.
1.2.2.3f	Assign a Chief Privacy Officer (CPO) to oversee the NASA-wide privacy program. The Chief Privacy Officer was formerly called the Privacy Program Manager.
1.2.2.3g	Assign a NASA Privacy Act Officer (PAO) responsible for oversight of NASA's compliance with the Privacy Act.
1.2.2.3h	Advise senior NASA officials concerning their responsibilities to protect privacy information.
1.2.2.3i	Evaluate legislative, regulatory, and other guidelines and policies related to privacy.
1.2.2.3j	Ensure that a Privacy Threshold Analysis (PTA) is conducted for any new, or significantly changed, applications, websites, information systems (including third party applications and information systems and collections of information provided for by external service providers who are collecting information on behalf of NASA), and all non-electronic information collections to determine whether there are any privacy implications or other regulatory compliance requirements Guidance for conducting PTAs is in ITS-HBK-1382.03-01, Privacy- Collections, PIAs, and SORNs.
1.2.2.3k	Ensure when initial assessments via the PTA process calls for the completion of a full Privacy Impact Assessment (PIA), one will be initiated and completed, in accordance with ITS-HBK-1382.03-01, prior to actively collecting any information.
1.2.2.3l	Reviews and approves PIAs.
2.2.2.1a	Ensure the establishment and maintenance of the NASA Master Privacy Information Inventory (MPII).

2.2.2.1b	Work with the SAISO to ensure the information system inventory required by NPR 2810.1, Security of Information and Information Systems, includes information on data processing systems processing PII.
2.3.2.1a	Establish Agency policy, requirements, and process for conducting PTAs and/or PIAs for new or revised applications and information systems to limit the identification of individuals.
2.3.2.1b	Assess the impact of technology on privacy and the protection of personal information.
2.3.2.1c	Evaluate and approve or disapprove all completed PIAs.
2.3.2.1d	Ensure that data is disposed of at the Agency level according to NRRS 1441.1, NASA Records Retention Schedules, NPR 2810.1, and NPR 2810.7.
3.2.2.1a	Ensure NASA users complete training and education on their privacy responsibilities, including acceptable rules of behavior, when and how to report privacy related incidents, and consequences for violating this NPR.
3.2.2.1b	Oversee the mandatory annual privacy training program.
3.2.2.1c	Oversee a privacy awareness program.
3.3.2.2	The SAOP shall update NASA senior management on the status of Agency performance in meeting privacy goals and objectives.
3.3.3.2a	Ensure external reporting requirements are met.
3.3.3.2b	Respond to external reporting requirements.
3.3.3.2c	Approve NASA's privacy reports required by OMB and 44 U.S.C. § 3551.
3.3.3.2d	Develop and maintain a privacy reviews schedule.
3.4.2.1a	Ensure policies and processes for filing and managing privacy complaints and inquiries are developed and maintained.
3.4.2.1b	Ensure that complaints are recorded, tracked, and addressed.
3.5.2.1	The SAOP shall outline the consequences and penalty guidelines related to privacy violations.
3.6.2.1a	Ensure policies and procedures for redressing misuse or mishandling of PII and for correcting inaccuracies are maintained. The SAOP will ensure that the policies follow these guidelines: (1) In accordance with the Plain Writing Act of 2010, 5. U.S.C. § 301, be in plain language and easy to read and understand. (2) Explain the right of redress. (3) Explain the process for complaining, seeking redress, and/or appealing adverse decisions. (4) Provide a general timeline for the redress process. (5) Identify the privacy policy related to PII being collected, processed, or

	(5) Identify the privacy policy related to PII being collected, processed, or maintained.
3.6.2.1b	Permit individual access to the Privacy Act SOR, in order to amend those Privacy Act records, as permitted in accordance with 14 CFR pt. 1212.
3.6.2.1c	In accordance with the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, Pub. L. 116-50, 133 Stat. 1073 (2019): (1) Ensure the ability for NASA to accept remote identity-proofing and authentication for the purposes of allowing an individual to request access to their records or to provide prior written consent authorizing disclosure of their records under the Privacy Act. (2) Ensure the ability for NASA to accept the access and consent forms from any individual properly identity-proofed and authenticated remotely through digital channels for the purpose of individual access to records or for authorizing disclosure of the individual's records to another person or entity, including a congressional office.
3.7.2.1a	Ensure Rules of Behavior for privacy are outlined within this NPR and maintained in the associated privacy handbook, ITS-HBK-1382.09-01.
3.7.2.1b	Ensure that awareness and training materials include information on privacy Rules of Behavior.
4.2.2.2a	Limit the collection of PII to that which is legally authorized, consistent with Federal and NASA privacy requirements, and to the minimum extent necessary.
4.2.2.2b	Ensure that PII is collected only when necessary for the proper performance of NASA’s functions and mission support.
4.2.2.2c	Conduct annual review activities to reduce or eliminate unnecessary collections of PII.
5.2.2.1a	Establish a Data Integrity Board that is responsible for approving, overseeing, and coordinating the matching program before any ISO may engage in a computer matching program as defined by the Privacy Act.
5.2.2.1b	Provide guidance on computer matching agreements.
5.4.2.1	The SAOP shall provide guidance on the use of Privacy Act Statements.
5.5.2.1a	Provide guidance on the development and publication of SORNs in such way that limits the formulation of inferences about individuals’ behavior or activities.
5.5.2.1b	Review and issue all SORNs for publication in the Federal Register.
5.6.2.2a	Ensure the NASA Web Privacy Policy: (1) Includes description of the information being collected. (2) Includes the purpose for the collection. (3) Includes the official use of, or need for, the collected information. (4) Specifies what information NASA collects automatically (e.g., user’s internet protocol (IP) address, location, and time of visit) and identifies the use for which it

	is collected (e.g., site management or security purposes). (5) Informs visitors as to whether their provision of the requested information is voluntary. (6) Informs visitors on how to grant consent for the use of voluntarily provided information. (7) Informs visitors on how to grant consent for NASA to utilize the information that the website collects for a use other than statutorily mandated or authorized routine uses under the Privacy Act. (8) Notifies visitors of their rights under the Privacy Act for SOR. (9) Incorporates information to meet the requirements of 15 U.S.C. §§ 6501-6506, where needed. (10) Includes information on the redress mechanism. (11) Notifies visitors as to how the Agency handles unsolicited e-mail, including the fact that the sender's privacy is not guaranteed.
5.6.2.2b	Disclose, in the applicable NASA Web Privacy Policy, a third party's involvement in Agency applications when they are embedded within a NASA website.
5.7.2.1a	Ensure the NASA Privacy Policy describes the use of third-party websites and applications, as outlined by OMB.
5.7.2.1b	Evaluate and approve or disapprove waivers for web measurement and customization technology that collects PII prior to use of that technology, as defined in ITS-HBK-1382.06, and annually thereafter.
6.2.2.1	The SAOP shall implement privacy policies and procedures to ensure the confidentiality and integrity of privacy information.
6.3.2.1a	Establish, implement, and publish Agency PII breach response and management policies and procedures in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
6.3.2.1b	Review, approve, or amend BRT recommended actions and notification plans.
6.3.2.1c	Advise NASA senior management on sensitive PII breaches and remediation progress.
6.3.2.1d	Activate an Agency BRT if the situation warrants a NASA-wide activation.
6.3.2.1e	Advise NASA senior management when notification and action plans need to be executed at a NASA-wide level.
6.3.2.1f	Ensure that all NASA users receive incident reporting training as outlined in Chapter 3 of this NPR.
1.2.2.3a	Provide overall responsibility and accountability for ensuring NASA's implementation of privacy information protections.
1.2.2.3b	Ensure that NASA is compliant with applicable Federal laws, regulations, policies, guidelines, and NASA privacy program requirements.